

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

HOMEWORK 1: GAUSSIAN INTEGERS I

This homework is due at the start of class on Wednesday Sep 13.

The first thing you should note is that there are very few problems. Nonetheless, get started right away, because it will take you a long time to come up with the solutions and write them up carefully. One of the goals of this course is to help you express your arguments cogently, concisely, and correctly (“**the three co’s**”). This is much harder than it sounds. **A certain number of points for the assignment go toward each of the co’s.**

1. Recall that an ordered pair (a, b) of real numbers determines a complex number $z = a + bi \in \mathbb{C}$ of modulus $|z| = \sqrt{a^2 + b^2}$ which is just the distance from z to 0 in the complex plane. Prove that for $z, w \in \mathbb{C}$, $|zw| = |z||w|$.

2. Prove that if $r, s \in \mathbb{Z}$ and $rs = 1$, then either $r = s = 1$ or $r = s = -1$.

3. Let $\mathbb{G}^\times = \{\alpha \in \mathbb{G} \mid \alpha\beta = 1 \text{ for some } \beta \in \mathbb{G}\}$ be the set of units (or invertible elements) in \mathbb{G} . Show that $\mathbb{G}^\times = \{\pm 1, \pm i\}$.

Hint: Show that $\alpha \in \mathbb{G}^\times \Rightarrow |\alpha|^2 = 1$, and then think geometrically about what this means.

4. Recall that $\gamma \in \mathbb{G}$ is a *Gaussian prime* if there do not exist $\alpha, \beta \in \mathbb{G} - \mathbb{G}^\times$ (i.e. α and β are non-invertible elements of \mathbb{G}) such that $\gamma = \alpha\beta$. Prove that $1 + i, 1 + 2i, 2 + 3i$ are Gaussian primes, and that $1 + 3i, 3 + 4i$ are **not** Gaussian primes.

5. Prove that 3, 7, and 103 are not sums of two integer squares. Is 1989 a sum of two integer squares? How about 2006?

6. Suppose you have access to a computer that given an integer k can decide quickly whether k is a perfect square or not. Devise and describe an algorithm (a procedure) for deciding whether a given natural number n is a sum of two integer squares.

Extra Credit Problem

A. Prove that if $m = a^2 + b^2$ and $n = c^2 + d^2$, with $a, b, c, d \in \mathbb{N}$, then there exist $e, f \in \mathbb{N}$ such that $mn = e^2 + f^2$. In other words, the product of two integers expressible as a sum of two squares is also expressible as a sum of two squares.